

Coming to Grips with the Growing Cyber Threat

February 2010



ON CYBER PATROL



It is almost impossible to understand the dangers that face our military, government, business and personal computer networks without being a high-level cyber security expert. What makes it even more difficult to fully grasp the threat is that you can't see it coming. There is no naval armada on the horizon or army marching towards us. This ever present danger is a constant, powerful, ceaseless attack that comes from all directions and from many different sources. According to recent statements by the Director of National Intelligence, David Blair, this already huge threat is "growing at an unprecedented rate."

But to a person who has not been the victim of a cyber attack or has not lost his or her identity or money due to online scams and traps, this threat is not a daily concern. Having a network brought down or data stolen is something that only happens to "the other guy." Often a person starts practicing good information assurance and cyber security only after they have become a victim. That's the equivalent of no longer walking through dark alleys in bad neighborhoods in strange cities only after having been mugged a few times. This behavior makes it much more likely that cyber attacks will be frightening successful.

Yet, without that personal experience of being a victim, it is very easy to see protecting against cyber threats as something less than a top priority, especially in a working world that is increasingly complex, fast paced and choked with information overload. There's just too much to do to worry about the "hidden dangers" of cyber threats.

There is plenty of effective technology available – for example, anti-virus software, secure access devices and network firewalls – that can significantly reduce the threat of a successful cyber attack. There are also a number of proven precautions and best business practices that, when used correctly and consistently, provide even more online security. But in the end it comes down to an individual person using these techniques. Unfortunately, because of the extent that government, business and personal networks are connected, a single person who does not protect access to data and networks can let in an attack that makes all other precautions useless.

If you think about that at a personal level, you might have a few moments of unease. Imagine being someone whose job it is to protect the critical networks that control our national security. It is almost impossible to see oneself in that position. One must wonder how they sleep well. Many don't.

However, in the middle of these looming cyber attacks, there is a way for you to sleep better at night. Whether you are in control of a single game system that has Internet access or in charge of a huge military network, just do your part. Use your training, don't cut corners, anticipate problems and keep your little corner of the Net safe and secure. Encourage and help everyone – fellow soldiers, co-workers, family and friends – to do the same. Lead by example when it comes to facing down this growing threat to our national networks and personal data. By making sure that your guardian link is not the one that is broken, you can inspire others to build and maintain an effective cyber defense.